SACSF/S4.16
GOVERNMENT STANDARD ON CYBER SECURITY

Secure Web Service Standard

Purpose

The purpose of this standard is to secure the web presence and information assets of the South Australian (SA) government.

Scope

This Standard supports the requirements of the South Australian Cyber Security Framework (SACSF) and applies to:

- South Australian Government public sector agencies (agencies), that is, administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown. Refer: *Public Sector Act 2009*.
- Suppliers to the South Australian Government and non-government personnel that provide services to agencies.

Scope inclusions

This standard applies to all public-facing web services hosted either on SA Government network infrastructure, by third-parties, or cloud service providers (e.g. AWS, Azure, Google) that are designed to be accessed and used by the public from the internet.

This includes all government websites and associated systems such as:

- Web applications that are developed or modified by agencies and/or third parties
- Commercial-off-the-shelf (COTS) software and mobile applications
- System components such as internet login portals, web servers, external application programming interfaces (APIs), and public facing modules.

Scope exclusions

This standard does not apply to:

- Web services that do not allow access from public networks.
- Internal web services hosted on the internal or external cloud infrastructure which only allow access from the SA government networks and accounts.

Table of contents

Standard

The standard requires agencies to implement security controls to safeguard web services based on risk. The risk profile of the web service determines the security category and the controls to be applied.

Baseline Security Controls

The following baseline security controls must be implemented for all web services to maintain a security baseline. Additional security controls must be implemented once the security category of each web service is determined.

#	Domain	Standard
1	Asset Register	• Web services and associated information assets must be identified and recorded in a register. • An Owner must be assigned to each web service in the register. The owner should be the business unit, individual or role responsible for the web service.
2	Compliance Requirements	• Legal, statutory, regulatory and contractual requirements relevant to the web services must be identified, documented and kept up to date. • The agency must maintain the compliance requirements of Payment Card Industry Data Security Standard (PCI-DSS) if the web service stores, processes, and/or transmits cardholder data. • The agency must maintain compliance requirements if the web services are subject to the Security of Critical Infrastructure (SOCI) Act.
3	Incident Response Readiness	• Developers and administrators must be trained to be able to recognise and report on a potential security incident related to the web service.
4	Information Classification	• The information asset classification, including confidentiality, integrity and availability, must be determined for the web services in alignment with the South Australian Information Classification System and Guideline for Integrity and Availability Classification using the SACSF. • The information asset classification must be documented in the register for the web services.
5	Risk Management	• Security risk assessments of web services must be undertaken and documented to identify the security risks associated with the acquisition, development, deployment, operation, and maintenance of the web services.
6	Supplier Management	• Security risk assessments of the web services must be undertaken and documented to identify the security risks that suppliers may introduce with the products or services they offering to the Agency associated with the web services. • Cyber security obligations to address identified risks must be documented within supplier agreements or contracts. Agencies must obtain assurance from suppliers that they have implemented controls to meet their cyber security obligations upon contract award and periodically thereafter.
7	Vulnerability Disclosure Program	• All newly commissioned web services must maintain processes to manage the identification and reporting of vulnerabilities in alignment with the SA Government Vulnerability Disclosure Program Policy.

Security Categories

Agencies must determine and document the category of each web service using the risk criteria in the table below.

A web service only needs to meet one criteria from a category for that category to apply.

All web services must apply the baseline security controls and the additional security controls up to the determined category as outlined in the Security Controls section.

For example, for a CAT-0 web service the baseline controls and the CAT-0 controls must be addressed. A CAT-1 web service must address the baseline, CAT-0 and CAT-1 controls, whilst a CAT-2 web service must address all security controls.

Category	Criteria
CAT-0 This category is for web services where the impact of a security breach is low, so only require minimum security controls.	• The web service does not process, store or transmit personal or sensitive information. • No security risks are identified, or the risks are accepted within risk appetite. • The web service does not support critical business operations. • The web service does not connect with any other Government systems, network or databases.
CAT-1 This category of for web services where the impact of a security breach may cause business interruption and data loss, so they require a medium level of security controls.	• The web service requires high level availability with minimum downtime or service outage. • The web service connects (via APIs or other interfaces that allow data transactions or logins) with other Government systems or databases that contain OFFICIAL information. • The wellbeing of individuals or the community may be negatively impacted if the web service were compromised or unavailable. • The web service is associated with low to medium level security risks.
CAT-2 This category is for the web services that are critical to the business and security breaches may cause disruption to important services or damage to information assets, and a high level of security controls are required.	• The web service processes, stores or transmits personal information and/or OFFICIAL: Sensitive information. • The web service supports critical business operations. • The web service processes, stores or transmits cardholder data and is subject to PCI DSS requirements. • The web service falls under the critical infrastructure asset classes of the SOCI Act. • The web service requires absolute availability with zero downtime or service outages. • Individuals or the community may suffer significant harm if the web service were compromised or unavailable. • The web service is associated with high to extreme level security risks. • There are direct connections and communication (via APIs or other interfaces that allow data transactions or logins) with other Government internal infrastructure, systems or databases that contain OFFICIAL: Sensitive information and/or above.

Security Controls

The following security controls must be implemented for all web services based on their security category.

#	Control Area	Category	Standard Requirements
1	Awareness and Training	CAT-0	None
		CAT-1	Agencies must train relevant employees, contractors and third-party service providers on: ○ The policies and procedures related to the web services usage and maintenance ○ Their roles and responsibilities in securing web services within the agency ○ How to properly store, transfer, archive, and destroy data related to web services.
		CAT-2	Agencies must conduct role-specific security awareness and skills training. Examples include: ○ Secure system administration courses for web service administrators ○ OWASP Top 10 vulnerability awareness and prevention training for web service developers ○ Advanced social engineering awareness training for high-profile users.
2	Backup and Restoration	CAT-0	Backups of web services data and configuration settings must be performed and retained with a frequency and retention timeframe in accordance with agency's business continuity requirements.
		CAT-1	• Backups must be retained in a secure and resilient manner, such as offline backup facilities, or online in a non-rewritable and non-erasable manner • Backup and restoration processes must be tested annually.
		CAT-2	• Backups of web services data and configuration settings must be performed daily, or more frequently, based on the sensitivity of the data, and stored for at least three months • Backups must be protected with equivalent controls to the original data. Example implementations include encryption and data separation, based on the security requirements • Backup and restoration processes must be tested at least twice a year for a sampling of in-scope web services.
3	Change Management	CAT-0	Changes to web services and associated infrastructure must be subject to the agency's change management procedures.
		CAT-1	As above

Security Controls

The following security controls must be implemented for all web services based on their security category.

#	Control Area	Category	Standard Requirements
		CAT-2	Changes to web services must maintain formal records of change requests, approval and testing results.
4	Cloud Computing	CAT-0	A security risk assessment must be undertaken before implementing any cloud services associated with the web services (including SaaS, PaaS, IaaS).
		CAT-1	As above
		CAT-2	Formal independent assurance reports (e.g. Service Organization Control 2 (SOC 2) report) relating to the risks associated with the service are obtained prior to the acquisition and on an annual basis for cloud services providing: ○ Critical services ○ Services with high availability or integrity requirements ○ Services storing sensitive information or higher ○ Services with a moderate or higher risk profile.
5	Configuration Management	CAT-0	A secure configuration process for web services must be established and documented to guide the configuration and hardening of all web services[1].
		CAT-1	As above
		CAT-2	A dedicated hardening standard must be developed for web services operating within the agency environment to outline the security configuration benchmarks and specific security controls for the system and infrastructure components.
6	Data Lifecycle Management	CAT-0	None.
		CAT-1	Data flows and the critical datasets of the web service must be identified and documented. The data flows documentation must be reviewed and updated annually, or when significant changes occur

[1] For examples of configuration management and hardening, see the ACSC Information Security Manual at www.cyber.gov.au, or OWASP.

Security Controls

The following security controls must be implemented for all web services based on their security category.

#	Control Area	Category	Standard Requirements
			A data management process must be established and maintained. The process should address data sensitivity, data ownership, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the web service Web service data stored in information systems, devices or in any other storage media must be deleted when no longer required.
		CAT-2	Data masking must be used for all sensitive data (e.g. personal information) in accordance with the agency's policy, business requirements, and applicable legislation.
7	Identity and Access Management	CAT-0	• Default accounts on web services, such as root, administrator, and other pre-configured vendor accounts must be disabled, or the password changed • Administrative access to the web services must only be granted to the personnel who require it to perform their job activities, and the access must be revoked immediately once there is no longer a specific business need for it • Access of terminated personnel must be revoked within defined timeframes • Reviews of administrative user access must be performed at least every six months • All administrative access of web services from public networks, where supported, must enable multi-factor authentication (MFA).
		CAT-1	• All users must have unique accounts providing traceability of actions within the web services • Reviews of general user access must be performed at least annually. Administrative user access reviews must be performed at least every three months • Dormant accounts must be deleted or disabled after a period of 45 days of inactivity, where supported. Terminated user's access must be revoked within defined timeframes • Restrictions must be applied to administrator accounts of web services to disable activities such as internet browsing, email, and productivity suite use, and be separate from the user's primary, non-privileged account • Password standards (complexity, minimum length, maximum age) for administrative accounts must be documented and implemented on all web services.
		CAT-2	• Access of terminated personnel must be revoked immediately upon departure • Reviews of administrative user access must be performed at least every three months

Security Controls

The following security controls must be implemented for all web services based on their security category.

#	Control Area	Category	Standard Requirements
			• MFA should be enabled by default to authenticate all users, including non-government users, where supported • Role-based access control for the web services should be defined and maintained, through determining and documenting the access rights necessary for each role to successfully carry out its assigned duties • An inventory of service accounts must be maintained. The inventory, at a minimum, must contain the owner, next review date, and purpose of the accounts • Service account reviews must be performed to validate that all active accounts are authorised, on a recurring schedule at a minimum quarterly, or more frequently.
8	Incident Response Readiness	CAT-0	None
		CAT-1	• An incident response process must be established, maintained, and tested at least annually • Key roles and responsibilities for incident response must be defined • Establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to web services security events • Mechanisms to communicate and report during a security incident must be defined, which include internal and external communication channels (e.g. with customers, public, and third parties).
		CAT-2	Incident response exercises and/or scenarios must be held at least annually for key personnel involved in the incident response process to prepare for responding to web services security incidents.
9	Logging and Monitoring	CAT-0	• Administrative account actions on the web service must be logged. • Audit logs of the web service must be logged and retained per the agency's logging and monitoring process • Time synchronisation should be standardised for logging.
		CAT-1	• Logs that record activities, exceptions, faults and other relevant events must be produced, stored, protected and analysed. Logs must be retained for a minimum of 90 days • The logs must contain essential event information, such as event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation

Security Controls

The following security controls must be implemented for all web services based on their security category.

#	Control Area	Category	Standard Requirements

			• Time synchronisation must be standardised for logging
			• The following logs related to the web service must be collected, where appropriate and supported:
			  ○ Web service server event logs
			  ○ Administrator workstation event logs
			  ○ Web service firewalls and network gateway logs
			  ○ Web service application audit logs
			  ○ Command-line audit logs, such as audit logs from PowerShell, BASH, and remote administrative terminals
			  ○ DNS query audit logs
			  ○ URL request audit logs.
			• Reviews of audit logs should be conducted to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

		CAT-2	• Security event alerting across web services should be centralised for log correlation and analysis. Best practice implementation requires the use of a Security Information and Event Management (SIEM) solution. Web services should be configured to send event logs to the centralised logging facility as soon as possible after each event occurs • Third party service provider logs should be collected where supported. Examples include collecting authentication and authorisation events, data creation and disposal events, and user management events that occur within a third party environment associated with the web services • Automated security incident response procedures may be implemented through a Security Orchestration, Automation and Response (SOAR) solution to resolve incidents more efficiently.
10	Network Communications	CAT-0	• Network and Architecture diagram(s) for the web services must be documented to understand the end-to-end information flows of the web services • The security of web services network infrastructure must be managed and maintained. Examples include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS).
		CAT-1	• Architecture diagram(s) and/or other network system documentation related to the web service must be maintained, reviewed, and updated annually, or when significant changes occur

Security Controls

The following security controls must be implemented for all web services based on their security category.

#	Control Area	Category	Standard Requirements
			• Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the agency and between the agency and other parties • Where web services connect to StateNet, the connections must comply with the StateNet Conditions of Connection. • Information flows associated with web services must be documented, which include: • The type of information • The classification of the information • Who the information is being exchanged with • The controls in place to protect the information.
		CAT-2	• Risk assessments must be performed for all information flows associated with critical web services, and appropriate security controls implemented. Information flow risk assessments must be reviewed annually • Application layer filtering to the web services should be performed. Examples include a filtering proxy, Web Application Firewall (WAF), or Secure Web Gateway (SWG) • Segregation must in place to isolate web services infrastructure, such as networks, data storage and servers. Web services isolation must be tested periodically.
11	Penetration Testing	CAT-0	• Penetration tests must be performed on the web service prior to the deployment and when any major change is made to detect exploitable vulnerabilities through a qualified party • Penetration test findings must be remediated based on the agency's policy and criticality of the findings.
		CAT-1	• Periodic penetration tests must be performed based on the agency testing program schedule.
		CAT-2	• Periodic internal and/or external penetration tests must be performed on the web services, based on program requirements, no less than annually.
12	Physical Security	CAT-0	• Physical security measures must be in place to protect the physical components (if applicable) of the web service.

Security Controls

The following security controls must be implemented for all web services based on their security category.

#	Control Area	Category	Standard Requirements
		CAT-1	As above
		CAT-2	As above
13	Resilience and Service Continuity	CAT-0	None
		CAT-1	• Business continuity readiness must be planned, implemented, maintained, and tested based on the agency's business continuity objectives and availability requirements • Web service recovery plans aligned to the outage limits identified in business impact assessments must be in place.
		CAT-2	• The web service recovery plans must be tested periodically as part of the assurance activities performed by agency. Business continuity and IT service recovery testing should include testing against cyber security scenarios • Redundancy must be built into systems commensurate with the system availability requirements identified as part of the business impact assessments.
14	Software Acquisition and Development	CAT-0	• Secure design principles must be applied in web services development projects to adapt security best practices and minimise the attack surface • Outsourced development of web services must be supervised • Software development, testing and production environments must be segregated for all web services.
		CAT-1	• Security requirements must be identified, specified, and approved when developing or acquiring web services. This includes the concept of least privilege, explicit error checking, and minimising the attack surface (e.g. turning off unprotected ports and services, session timeout, removing unnecessary programs and files, and renaming or removing default accounts) • Secure engineering principles must be established, documented, and applied to web service development activities. This should include the secure coding practices such as REST API Security Principles, OWASP Web Service Security Cheat Sheet, etc.

Security Controls

The following security controls must be implemented for all web services based on their security category.

#	Control Area	Category	Standard Requirements
			• Security testing processes must be defined and implemented in the Software Development Life Cycle (SDLC). Industry best practice such as the OWASP Web Security Testing Guide should be considered when developing a security testing program.
		CAT-2	• Code reviews must be performed by suitably skilled personnel prior to implementation • Code reviews should be performed by an independent third-party prior to implementation.
15	Supplier Management	CAT-0	• Supplier contracts must include security requirements, such as minimum security capabilities, security incident and/or data breach notification and response, data ownership, data encryption requirements, availability requirements, security audit rights, and data disposal commitments • Assurance must be obtained from suppliers that they have implemented controls to meet their cyber security obligations upon contract award and periodically thereafter.
		CAT-1	• A security policy must be established and maintained that addresses the security requirements of third party web services providers. This should include inventory, assessment, monitoring, and decommissioning requirements.
		CAT-2	• Agencies must obtain independent assurance from suppliers that they have implemented controls to meet their cyber security obligations upon contract award and annually thereafter • Agency must assess supplier risk, and review assessment reports, such as SOC 2 and PCI Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Suppliers should be reassessed annually, at a minimum, or with new and renewed contracts • Supplier performance and risks must be monitored, which may include periodic reassessment of service provider compliance, monitoring web services release notes, and dark web monitoring • Suppliers must be securely decommissioned. Examples include user and service account deactivation, termination of data flows, and secure disposal of data within service provider systems.
16	Use of cryptography	CAT-0	Data must be encrypted in transit. Example implementations should include Transport Layer Security (TLS), HTTPS, and Open Secure Shell (OpenSSH).

Security Controls

The following security controls must be implemented for all web services based on their security category.

#	Control Area	Category	Standard Requirements
		CAT-1	Rules for the effective use of cryptography, including cryptographic key management, must be defined and implemented for the web service. The ACSC Guidelines for Cryptography should be considered for selecting cryptographic protocols and algorithms.
		CAT-2	• Sensitive data must be encrypted at rest. Example implementations include implementing full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition • Backup copies of sensitive data must be encrypted to prevent unauthorised access.
17	Vulnerability and Patching Management	CAT-0	• Information about technical vulnerabilities of web services in use must be obtained. Exposure to identified vulnerabilities must be evaluated and appropriate measures must be taken.
		CAT-1	• Vulnerability scans of web services should be performed on a fortnightly, or more frequent, basis. The vulnerability scanners should have an up-to-date vulnerability database and should be automated • Patches, updates, or vendor mitigations for security vulnerabilities in web services must be applied within one month of release • Web services that are no longer supported by vendors must be terminated or segregated from other web services.
		CAT-2	• Vulnerability scans of web services must be performed on a weekly, or more frequent, basis. • Patches, updates, or vendor mitigations for security vulnerabilities in web services must be applied within two weeks of release, or within 48 hours if an exploit exists.

Application Programming Interfaces (API) Security

The following security principles and best practices must be applied during the development and use of APIs.

After the controls below, there is a list of external resources for developers and system owners to use for up-to-date best practices in API security.

#	Controls	Description
1	Always Use HTTPS	• HTTPS must be used to protect authentication credentials in transit, including passwords, API keys or JSON Web Tokens (JWTs) • For highly privileged web services, mutually authenticated client-side certificates should be used to provide additional protection.
2	Use Password Hash	• Passwords must always be hashed to protect the credentials from unauthorised access or disclosure • The algorithms in use to hash passwords must be secure and effective, such as PBKDF2, bcrypt, and scrypt.
3	Never expose information on URLs	• Sensitive information such as usernames, passwords, session tokens, and API keys must not appear in the URL, as this can be captured in web server logs, which makes them easily exploitable.
4	Consider OAuth	• OAuth should be implemented for API authentication. Example implementations include the OAuth 2.0 authorisation framework, which enables a third-party application to obtain limited access to web services.
5	Consider Adding Timestamp in Request	• A request timestamp should be added along with other request parameters to prevent basic replay attacks from attackers who are trying to brute force without changing the timestamp • Web services should only accept the request if it is after a reasonable timeframe (i.e. 30 seconds).
6	Input Parameter Validation	• Request parameters (e.g. numbers, booleans, dates, times or fixed data ranges) and input (length / range / format and type) must be validated before reaching application logic • Strong validation checks must be implemented, and the requests must be rejected immediately if validation fails

		• Language specific validation / sanitation libraries or frameworks should be used to develop validation checks • Input validation failures should be logged to identify someone who is performing cyber attacks or exploration attempts • In API response, relevant error messages and examples of correct input format should be sent to improve user experience. For example, reject requests exceeding the size limit with HTTP response status *413 Request Entity Too Large*.
7	API Keys	• API keys for every request must be required to the protected endpoint • API key must be revoked if the client violates the usage agreement • If requests are coming in too quickly, *429 Too Many Requests* HTTP response code should be returned • API keys should not be relied on exclusively to protect sensitive, critical or high-value resources.
8	Restrict HTTP methods	APIs must apply an allow list of permitted HTTP methods e.g. GET, POST, PUT, and reject all requests that are not matching the allow list with HTTP response code *405 Method not allowed*
9	Validate Content Types	• All supported content types in the APIs must be documented. • APIs should validate request content types, by the following: • Reject requests containing unexpected or missing content type headers with *HTTP response status 406 Unacceptable* or *415 Unsupported Media Type* • For XML content types ensure appropriate XML parser hardening • Avoid accidentally exposing unintended content types by explicitly defining content types. • APIs should send safe response content types, but not simply copy the *Accept* header to the *Content-type* header of the response and reject the request (ideally with a *406 Not Acceptable response*) if the Accept header does not specifically contain one of the allowable types.
10	Management Endpoints	• Management endpoints should not be exposed via the internet • If management endpoints must be accessible via the internet, users must use a strong authentication mechanism (e.g. MFA) • Management endpoints should be exposed via different HTTP ports or hosts preferably on a different NIC and restricted subnet

		• Access to these endpoints should be restricted by firewall rules or use of access control lists.
11	Error Handling	• Generic error messages should be responded (i.e. avoid revealing details of the failure unnecessarily) • Technical details (e.g. call stacks or other internal hints) must not be passed to the API clients.
12	Audit Logs	• Audit logs should be documented for security related events, which include token validation errors, failed authentication attempts, denied access, and input validation errors • Logs should be written using a format suited to be consumed by a log management solution, and should include enough detail to identify the malicious actor • Logs should be handled as sensitive data, and their integrity should be guaranteed at rest and in transit • Log data should be sanitised beforehand to avoid log injection attacks.
13	Security Headers	• Security headers should be included in all API responses to prevent sensitive information from being cached, protect against cyber attacks, and required HTTPs connections. Example headers include *Cache-Control: no-store, Content-Security-Policy: frame-ancestors 'none', Strict-Transport-Security, and X-Frame-Options: DENY*, etc. • Other security headers and example implementations should be applied to APIs where possible. The best practices of security headers could be found at OWASP Secure Headers Project | OWASP Foundation
14	Rate Limiting	Rate limiting and throttling policies should be applied to prevent abuse of API. Ensure appropriate alerts are implemented and respond with informative errors when thresholds are nearing or have been exceeded.

15	Access Control	• A proper authorisation mechanism must be implemented to check if the logged-in user has access to perform the requested action
		• The enforcement mechanism(s) should deny all access by default, requiring explicit grants to specific roles for access to every function
		• Administrative functions should be implemented inside a regular controller for authorisation checks based on the user's group and role
		• Where possible, the following access control mechanism should be implemented:
		  ○ multi-factor authentication.
		  ○ anti-brute force mechanisms

		○ account lockout / captcha mechanism ○ weak-password checks.
16	Avoid Mass Assignment / Autobinding	• Functions that automatically bind a client's input into code variables or internal objects should not be used • Whitelist only the properties that should be updated by the client and blacklist properties that should never be accessed by clients • Use the read only property set to true in object schemas for all properties that can be retrieved through APIs but should never be modified • Schemas, types, and patterns that the API will accept in requests should be defined at design time and enforced them at runtime.
17	Asset Management	• API hosts must be documented with the important aspects of each one of them, focusing on the API environments (e.g. production, staging, test, development), and who have network access to the hosts (e.g. public, internal, partners) and the API versions • Integrated services must be documented with the important aspects such as their roles in the system, what data is exchanged (data flows), and data sensitivity • All aspects of the API should be documented, such as authentication, errors, redirects, rate limiting, Cross-Origin Resource Sharing (CORS) policy and endpoints, including their parameters, requests, and responses • When newer versions of APIs and security improvements are available, risk assessments should be performed to make the decision of the mitigation actions required for the older versions.
18	Data Security	• Production data should not be used with non-production API deployments. If this is unavoidable, the endpoints should get the same security treatments as the production ones • Data should be encrypted during transit and at rest • Responses from the API should be reviewed to make sure they contain only legitimate data • API calls returning personal information should be reviewed to see if these responses pose a security issue or violate the privacy policy • A schema-based response validation mechanism should be implemented to define and enforce data returned by all API methods, including errors.

External References resources for developers and system owners to use for up-to-date best practices in API security:

- REST API Security Essentials
- Australian Government - API Design Standard
- OWASP Cheat Sheet Series - REST Security Cheat Sheet
- OWASP API Security Project
- Australian Government - National API Design Standards (NAPIDS) – GitHub

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this standard. There is no specific impact on Aboriginal people.

Related documents

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls
- South Australian Cyber Security Framework (SACSF)
- South Australian Protective Security Framework (SAPSF)
- StateNet Conditions of Connection (available internal to government only)
- Australian Cyber Security Centre - Information Security Manual (ISM)
- South Australian Information Privacy Principles (IPPS) Instruction
- Security of Critical Infrastructure Act 2018
- Payment Card Industry Data Security Standard (PCI-DSS)
- Preventing Web Application Access Control Abuse (ACSC, CISA, NSA)

Definitions

Term	Definition
MUST	This word, or the terms "REQUIRED" or "SHALL", mean that the defined security controls are mandatory for the compliance of this standard.
SHOULD	This word, or the adjective "RECOMMENDED", mean that there may exist compensating security controls to ignore the defined security controls, or the associated security risks are accepted based on Agency's defined risk appetite and management decisions.
MUST NOT	This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful.
Web service	A service used to communicate between two devices on a network – e.g. web server, website, web application.
Web server	The infrastructure where a web site or web application runs. It may be dedicated hardware or virtualised and includes software components such as the operating system. It may be hosted on-premise, on third party infrastructure, or on cloud infrastructure (e.g. AWS or Azure).
Website	A collection of web pages and related content that is identified by a common domain name and published on at least one web server.

Term	Definition
Web application	Application software which runs on a web server and is accessed using a web browser or software. Web applications are generally interactive and may connect to a backend database or another application server.
Role-based Access Control (RBAC)	A mechanism to define access rights based on users' job roles and privileges. This control makes it simple to perform account provisioning and user onboarding, enable separation of duties, and restrict access to systems and resources in a more granular manner.
Multi-factor Authentication (MFA)	An authentication control that uses two or more proofs of identity to grant user access, rather than relying on single set of username and password.
Application Programming Interface (API)	A software interface with a defined set of rules that enables different applications to communicate with each other.

DOCUMENT CONTROL

Approved by: CIO Steering Committee	
Contact: Chief Information Security Officer	
Division: Office of the Chief Information Officer	Compliance: Mandatory
Review number: V2.0	Date of approval: 23 August 2023
Next review date: 23 August 2024	Original approval: July 2014 (DPC/S4.14 and DPC/S4.15)